

EXHIBIT 3

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL.,)
)
Plaintiffs,)
) Civil Action No.
vs.)
) 1:17-CV-2989-AT
BRAD RAFFENSPERGER, ET AL.,)
)
Defendants.)

VIRTUAL VIDEOTAPED 30(b)(6) DEPOSITION OF
SANFORD MERRITT BEAVER

Thursday, March 10, 2022

9:09 a.m.

VOLUME II (Pages 260 - 439)

Robin K. Ferrill, CCR-B-1936, RPR

1 VIRTUAL VIDEOTAPED 30(B)(6) DEPOSITION OF

2 SANFORD MERRITT BEAVER

3 Thursday, March 10, 2022

4 THE VIDEOGRAPHER: We are on the record
5 March 10th, 2022 at approximately 9:09 a.m.
6 Eastern time. This will be Volume II to the
7 30(b)(6) videotaped deposition of the Office of
8 Secretary of State. Representative today will
9 be Sanford Merritt Beaver.

10 Would counsel please identify themselves
11 and who they represent for the record.

12 MR. DENTON: Morning. This is Alexander
13 Denton, here on behalf of the State Defendants.

14 I'll also announce at this time, because I
15 believe his microphone is not connected, that
16 Mr. Pico-Prats, also with our firm, is here on
17 behalf of the State Defendants.

18 MR. CROSS: David Cross of Morrison &
19 Foerster on behalf of Curling Plaintiffs.

20 MR. HAVIAN: Eric Havian, Constantine
21 Cannon on behalf of Coalition for Good
22 Governance.

23 MS. MARKS: This is Marilyn Marks. I'm a
24 Plaintiff's representative for Coalition for
25 Good Governance.

1 MR. TYSON: Good morning. Bryan Tyson for
2 the State Defendants.

3 MR. MILLER: This is Carey Miller, also
4 here for the State Defendants.

5 MR. LOWMAN: This is David Lowman for the
6 Fulton County Defendants.

7 MS. GREENHALGH: Susan Greenhalgh,
8 consultant to Coalition for Good Governance.

9 MS. CONNORS: This is Jill Connors,
10 paralegal for Ichter Davis for Coalition
11 Plaintiffs.

12 THE VIDEOGRAPHER: Thank you.

13 Would the court reporter please swear in
14 the witness.

15 SANFORD MERRITT BEAVER,

16 called as a witness, having been duly sworn
17 by a Notary Public, was examined and testified as
18 follows:

19 EXAMINATION

20 BY MR. CROSS:

21 Q. Good morning, Mr. Beaver.

22 A. Morning.

23 (Plaintiffs' Exhibit 1, Fortalice Solutions
24 Technical Assessment Prepared for Secretary of
25 State Georgia, DRAFT - May 19, 2020, Bates

1 deposition?

2 A. I went through the different documents that
3 were sent to me. There was 20 of them. Nineteen
4 were of the same document but different versions,
5 apparently. My guess, different versions. I'm
6 guessing they were all working copies of whoever was
7 building this document.

8 So I went through them. I didn't do a
9 comparison, but I did go up through most of them.
10 After -- after a while they all looked similar.

11 And then there was one other document,
12 which was the red hat report.

13 Q. What's the red hat report?

14 A. A red hat report is basically a report from
15 Fortalice where they take the stance of a malicious
16 attacker to use whatever resources they have to try
17 to breach our system.

18 Q. And do you remember the date, timing of
19 that report?

20 A. I would have to go look at it. I do not.

21 Q. What do you remember about that report?

22 A. Essentially, they talked a lot through
23 their -- the different steps they went through to
24 breach the system from the outside. After going
25 through -- and they documented a number of different

1 approaches they took.

2 At, I think, on the end of -- I think it
3 was Page 6, they defined that they were not able to
4 breach the system with any resources or expertise
5 that they had, and so they moved on to a admitted
6 breach. Admitted breach, meaning we gave them access
7 to a machine as if they were able to breach so they
8 could go into a Phase II to look into moving around
9 our system.

10 Q. When you say "gave them access to a
11 machine," how did you do that?

12 A. We gave them username and password to a
13 computer that was on our network.

14 Q. And why did you give them that access?

15 A. Because they could not get into our system.
16 And the next level of testing was to simulate a
17 breach that had -- potentially had happened, what the
18 potential person could do if they were able to get
19 in. But since they weren't able to breach the
20 system, we make the assumption that "Okay. Let's
21 assume that you are able to get in. Let's give you
22 access as if you were able to breach and then see
23 what you can do." It's a typical exercise when you
24 do red hat.

25 Q. Sorry. You said it's a typical exercise

1 when you do that, and I think I interrupted you.

2 What do you mean by that?

3 A. So red hat is testing basically all your
4 layers of defense in security. If we stop them on
5 the outside so they can't get in, then all we know
6 about our system is that we have got a really good
7 external security layer.

8 But over time things change. People
9 find -- and systems find other vulnerabilities. And
10 if somebody was able to exploit a vulnerability that
11 nobody knew about, then they might be able to get
12 into the system. We still want to know if somebody
13 got into the system what could happen.

14 So we allow somebody a red hat test to get
15 in as if they did breach the system so that they
16 could go to the next level of testing to see, once
17 they got in, what it would look like.

18 Q. And you said this is a typical type of
19 testing. What do you mean it's typical?

20 A. We do an assessment every year. And this
21 is the typical -- there is something called a blue
22 hat, a red hat and a purple hat. Those are security
23 terms for the types of external testing. Red hat is
24 the most aggressive attack.

25 Q. What's a blue hat test?

1 A. That is a -- basically where we give them
2 access to different points ahead of time so they can
3 test, but they know ahead of time how to get in.

4 Q. What's a purple hat test?

5 A. It's a blend of the two.

6 Q. Is the idea with these different types, the
7 red hat and the others, to try to simulate realistic
8 circumstances? You have some sense of
9 vulnerabilities in the real world with your actual
10 system. Is that kind of the idea?

11 A. Yes.

12 Q. The red hat report you said you looked at,
13 is there anything else you remember about it?

14 A. Not off the top of my head, no.

15 Q. Okay. And you said, if I understood you
16 right, so you looked at 20 documents. One was the
17 red hat report. The other 19 looked to be different
18 versions of the same report, which looks to be
19 Exhibit 1; is that right?

20 A. Correct. Exhibit 1 is an early version of
21 the -- an early draft. It's on the 19th. I think
22 the drafts go as far forward, if I remember, as the
23 25th.

24 Q. Of May? 25th of May?

25 A. Yes, I think it was.

1 A. That's a broad question. Voting system is
2 a lot of different pieces and parts. Which one --
3 what are you specifically asking about?

4 Q. (By Mr. Cross) So one of the responses the
5 State has made in response to this July 1 report from
6 Dr. Halderman is that, you know, some of the
7 vulnerabilities he finds, like, for example, the
8 ability to upload malware through a USB port on the
9 voting equipment, are you aware of any measures taken
10 by the Secretary's Office or by a county to increase
11 security around access to those ports or to the
12 machines?

13 A. I'm not aware. That doesn't mean it hasn't
14 been done.

15 Q. Are you aware of any measures taken by
16 Dominion to address vulnerabilities with their own
17 voting equipment since July of 2021?

18 A. I'm not aware.

19 Q. Do you know whether anyone at the
20 Secretary's Office has discussed Dr. Halderman's
21 report with anyone at Dominion? This report?

22 A. I'm not aware.

23 Q. If you wanted to know the answer to that,
24 who would you ask?

25 A. I might start with Gabe Sterling or Michael

1 Barnes.

2 Q. Do you know whether Secretary Raffensperger
3 has reviewed this July 1 report?

4 A. No, I am not aware.

5 Q. If you wanted to know, who would you ask?

6 A. I might ask him.

7 Q. Okay.

8 Okay. Do you know whether Jordan Fuchs has
9 reviewed the July 1 report from Dr. Halderman?

10 A. I'm not aware of anything about this report
11 with anybody at SOS.

12 Q. So as you sit here, you are not aware of
13 anyone at the Secretary's Office -- you can't
14 identify anyone who has read this report; is that
15 fair?

16 A. That's fair.

17 Q. Have you -- well, I guess to give it some
18 context, do you understand that this report has gone
19 to CISA at DHS?

20 A. (Unintelligible.)

21 Q. I'm sorry. There's some static.

22 A. I said other than you just telling me that.

23 Q. Can you hear me?

24 A. Can you hear me?

25 THE VIDEOGRAPHER: I'm getting some really

1 should be public? Publicly released?

2 A. I don't think that's my decision.

3 Q. Okay. But you are the Chief Information
4 Officer for the Secretary's Office. Do you have a
5 view from a cybersecurity perspective on whether this
6 report, which purports to identify numerous
7 vulnerabilities with the voting system, whether it
8 should be released publicly?

9 A. Anything that can adversely effect
10 security, in my opinion, shouldn't be released. You
11 are only reducing Georgia's ability to secure their
12 equipment and systems whenever security information
13 about an existing system is released. In my mind,
14 it's bad practice and just, you know, being ignorant
15 of cybersecurity.

16 Q. Last couple questions or couple points.

17 What are the industry-recognized benchmarks
18 that the Secretary's Office attempts to adhere to for
19 cybersecurity for the voting system, if any?

20 MR. DENTON: Object to form.

21 A. That is way too broad of a question.

22 MR. CROSS: Fair enough. Let me narrow it
23 down. Let's just focus on the Dominion
24 equipment, the BMDs, the printers, the scanners.

25 Q. (By Mr. Cross) What, if any,

1 than a day.

2 Q. (By Mr. Havian) So until yesterday, you
3 were not aware of Topic Number 10 at all; is that
4 correct?

5 MR. DENTON: Object to form.

6 Q. (By Mr. Havian) Just so I clarify, by
7 Topic 10, I'm referring to Topic Number 10 that's
8 stated in Exhibit 11 that you are looking at now.

9 A. Correct.

10 Q. Okay. So after you learned about Topic
11 Number 10 yesterday, you didn't have -- is it fair to
12 say you just didn't have sufficient time to speak
13 with others in the Georgia Secretary of State's
14 Office to see if anyone else might have information
15 on that topic? Is that fair?

16 A. That would be fair.

17 Q. If you did have more time to inquire, who
18 would you speak to about Topic Number 10 to find out
19 what the Georgia Secretary of State's Office knew
20 about it?

21 A. I would speak to probably the head of the
22 elections group, Blake Evans. Probably would speak
23 to my security person, although if he had heard of
24 anything -- I say person, my security manager -- if
25 he had heard something, he would have probably told

1 me.

2 So the fact that I didn't hear anything
3 from him, I know his answer. I might talk to Gabe
4 Sterling. I might talk to Michael Barnes. Those
5 would be my starting points.

6 Q. And who is the security person that you are
7 referring to?

8 A. Kevin Fisk.

9 Q. All right. So let me ask you a few other
10 questions, more general questions about Coffee
11 County.

12 First of all, are you aware that
13 Mr. Gabriel Sterling gave a deposition in this matter
14 as well?

15 A. I just heard about it. I have no details
16 on it.

17 Q. I'm going to read to you something that
18 Mr. Sterling said in his deposition and ask you
19 whether you agree with his statement or not.

20 Mr. Sterling testified, quote, "Physical
21 security is the -- obviously, the frontline of all
22 cybersecurity. And that's one of our main things we
23 have to worry about at all times. That's why we --
24 we work with the counties to make sure they have
25 these things in under lock and key," close quote.

1 event?

2 A. It depends on where it happens. If it
3 happens in the counties, Chris Harvey might have
4 heard of it. But he worked with the county to find
5 out what happened.

6 I mean, we will get messages from counties
7 saying that e-mails have been compromised and they
8 don't know whether or not they have hacked into the
9 system. And so the county level will go through and
10 send Chris Harvey a message saying this is what they
11 are doing to evaluate it. And then when they have
12 resolved what happened, they will let him know. And
13 if it doesn't deem that it was impacting our system,
14 he wouldn't let me know.

15 Q. All right. So -- and again, just so I
16 understand this correctly, if something happens at
17 the county level but it's an incident that is
18 deemed -- or rises to the level of an incident and
19 involves election security --

20 A. I will hear about it.

21 Q. What's that?

22 A. I will hear about it.

23 Q. You will hear about it. So in other words,
24 it can't just -- something that I've just described
25 can't be resolved properly at the county level and

1 the state has to get involved; is that fair?

2 MR. DENTON: Object to the form.

3 A. Traditionally, in the past, I have heard
4 about it if it -- if it truly has happened.

5 Q. (By Mr. Havian) Okay. And when you say --
6 I think you mentioned that you were describing the
7 process that Investigations gets involved. Can
8 you -- is there a specific department that you were
9 referring to there?

10 A. So we have an Investigation Department.
11 Frances -- Ms. Frances was heading that department.
12 So she -- she might get pulled in. If it is
13 something that needs more technical investigation,
14 that's why we use Fortalice to do our forensics work
15 there.

16 It all depends on the type of
17 investigation. It may be just something that
18 department heads can work through. If it's a county
19 level, the county is going to have to go through.
20 They're the ones that basically manage and own their
21 process.

22 Q. Okay.

23 Let's go back to Exhibit 13, the Harvey
24 memo for a moment.

25 A. Yes.

C E R T I F I C A T E

STATE OF GEORGIA)

) ss.:

FULTON COUNTY)

I, Robin Ferrill, Certified Court Reporter within
the State of Georgia, do hereby certify:

That MERRITT BEAVER, VOLUME II, the witness
whose deposition is hereinbefore set forth, was duly sworn
by me and that such deposition is a true record of the
testimony given by such witness.

I further certify that I am not related to any
of the parties to this action by blood or marriage; and
that I am in no way interested in the outcome of this
matter.

IN WITNESS WHEREOF, I have hereunto set my
hand this 25th day of March, 2022.



ROBIN K. FERRILL, RPR